



CONTACT: Mary Jane Collipriest, 202-224-5444, Washington, D.C. 20510

FOR IMMEDIATE RELEASE  
September 24, 2001

## **BENNETT INTRODUCES BILL TO PROTECT CRITICAL INFRASTRUCTURE THROUGH INFORMATION SHARING**

### ***CRITICAL INFRASTRUCTURE INFORMATION SECURITY ACT OF 2001 WILL STRENGTHEN ECONOMIC AND NATIONAL SECURITY***

**WASHINGTON, D.C.-** In the wake of the devastating terrorist attacks of September 11, 2001, Senator Bob Bennett (R-Utah) today introduced legislation to address a dangerous national security blind spot by encouraging two-way information sharing, and improve federal and private industry communication to help protect America from further physical or cyber attack.

"President Bush has warned us of the new fight ahead," said Bennett. "With more than 85 percent of critical infrastructure entities owned and operated by the private sector, voluntarily shared information leads to a more focused understanding of threats and empowers government, industry and private citizens to mitigate risk. Ultimately, this bill will help assure the reliable delivery of services critical to the nation's economy and security.

"On September 11, 2001, America suffered a fundamentally different type of attack. America's commercial airspace was weaponized and turned viciously against its financial defense establishments in an infrastructure attack. This senseless attack killed thousands and resulted in grave physical and financial loss."

Critical infrastructure includes key sectors such as financial services, telecommunications, transportation, energy, emergency services, and government essential services whose disruption or destruction would greatly impact the economy and national security. The rapid development of technology and its interconnectivity have made it easier to attack critical U.S. infrastructures with physical or computer based attacks than at any other time in history.

The Critical Infrastructure Information Security Act (CIISA), co-sponsored by Senator Jon Kyl (R-AZ), and developed earlier this year, is intended to increase the sharing of information and improve threat analysis for critical infrastructures. Information sharing between government and private sector industries will give critical infrastructures a fuller understanding of potential threats, greatly increasing their risk management potential.

Designed to increase the two-way sharing of information between the federal government and the private sector, the CIISA will accomplish the following:

- **Secure voluntarily shared critical infrastructure information**

The CIISA allows a critical infrastructure entity to voluntarily submit sensitive information, which would normally not be shared, to one of 13 designated federal agencies and request information be protected. Doing so means that specific information shared with a federal agency for analysis, warning or interdependency study will not be disclosed in response to a request under the Freedom of Information Act (FOIA).

FOIA is an essential element of transparent government. Initially enacted in 1966 for any person, including foreign citizens, partnerships, corporations, associations and foreign governments, FOIA allows presumptive access to existing, unpublished agency records on any topic. There are no limitations on FOIA even during times of war.

CIISA does not alter FOIA in any way and will protect voluntarily shared information without diminishing federal transparency by working within legally provided non-disclosure exemptions that protect information. Such information would not be in the public domain in the first place and if publicly released could disrupt, or compromise the security of critical infrastructure operations.

- **Provide critical infrastructure threats analyses**

CIISA requires that information and analyses from the federal government be shared back with the private sector in the form of notifications, warnings, and strategic analysis, while requiring federal agencies receiving the classified information to do the following: 1) analyze the information, 2) determine the tactical and strategic implications of such information, 3) identify interdependencies, 4) consider conducting further analysis in concert with other federal agencies.

Following this analysis, a federal agency may issue warnings regarding potential threats to individual companies, targeted industry sectors, the general public or other government agencies. Federal agencies must take appropriate actions to prevent disclosure of the source of any voluntarily submitted information.

CIISA also requires the president to designate an element within the Executive Branch to conduct strategic analysis of potential threats to critical infrastructure, develop strategic analysis capabilities, and submit a plan to the Governmental Affairs Committee detailing how the capabilities will be developed.

- **Protecting those who share information**

When competitors work closely together, antitrust concerns often surface. In order to promote the idea that security in a network oriented world is a shared responsibility and to encourage the private sector to lead in developing solutions to common security problems, CIISA provides a narrow antitrust exemption, not unlike that of the Information Readiness Disclosure Act or the Defense Production Act. Information Sharing and Analysis Organizations, formed solely for the purpose of gathering and analyzing critical infrastructure information to better understand problems, integrity and reliability of critical infrastructure, will be exempt from antitrust laws.

The antitrust exemption will not apply to conduct that involves or results in an agreement to boycott any person, to allocate a market, or to fix prices or output.

###